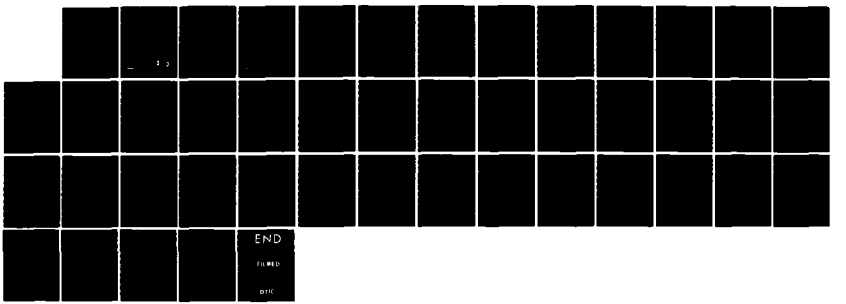
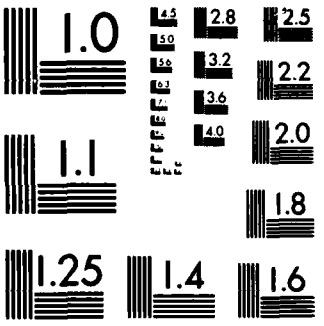
AD-A152 755 MILITARY COUNTERMEASURES TO TERRORISM IN THE 1980S(U) 1/1
RAND CORP SANTA MONICA CA T C TOMPKINS AUG 84
RAND/N-2178-RC

UNCLASSIFIED F/G 15/7 NL





A RAND NOTE

AD-A152 755

DTIC FILE COPY

MILITARY COUNTERMEASURES TO TERRORISM IN THE 1980s

Thomas C. Tompkins

August 1984

N-2178-RC

This publication was supported by The Rand Corporation as part of its program of public service.

Published by The Rand Corporation

A RAND NOTE

MILITARY COUNTERMEASURES TO TERRORISM IN THE 1980s

Thomas C. Tompkins

August 1984

N-2178-RC

Rand
1700 MAIN STREET
P.O. BOX 2138
SANTA MONICA, CA 90406-2138

PREFACE

This Note examines the countermeasures to terrorism undertaken by the four military services in the 1980s. These countermeasures can be categorized as either offensive (*counterterrorism*) or defensive (*antiterrorism*). A definitional and descriptive work supported by The Rand Corporation from its own funds, the study summarizes an effort undertaken by the Security and Subnational Conflict Program in its continuing research for the Department of Defense and other executive agencies of the U.S. government.

The discussion is based on data derived from the Rand Chronology of International Terrorism, a review of current literature on terrorism counteraction, and an examination of selected military countermeasures programs. The Note should be of particular interest to those agencies that interact with the military and so require an understanding of the services' various approaches to countering terrorism.

SUMMARY

The numerous terrorist attacks that have been made on U.S. military installations and personnel since 1980 have prompted the military to undertake certain countermeasures. These can be categorized as either offensive (*counterterrorism*) or defensive (*antiterrorism*). Each of the four major military services has approached the problem differently, although the Army and the Air Force have tended to run parallel tracks in their terrorism countermeasures. This Note outlines the terrorist threat to the U.S. military and identifies some critical elements of viable antiterrorism (AT) and counterterrorism (CT) programs, outlining both variances between the service programs and similarities among them. The results suggest that there is a need for central direction and control in the services' terrorism countermeasures.

Analyses of terrorist targeting indicate an apparent increase in premeditated attacks against U.S. military installations and individuals. The services have reacted to this trend by spending over $2 billion annually for physical security alone. The actual costs are not available, since the services have not specifically identified security costs in their budget requests (despite a recommendation by the General Accounting Office (GAO) that they do so).

Four elements are considered critical for effective AT or CT efforts:

- Credible, reliable, and timely intelligence.
- Proper education and training.
- Modern tactics and techniques.
- Up-to-date equipment and devices.

The problems of meeting the intelligence requirement have been compounded by the severe constraints imposed on U.S. intelligence agencies during the anti-Vietnam War era and also by a lack of communication between the intelligence community and the operators who need and use intelligence information. The Reagan Administration has

relaxed some of the intelligence-gathering constraints, however, and the communications problem may be helped by the assignment of operations personnel to an all-source information center, the creation of which was recommended by the Long Commission, following its investigation of the bombing of the U.S. Marine Corps headquarters in Beirut.

Education and training in countermeasures are conducted primarily by the Army and the Air Force. The Navy and the Marines generally use Army and Air Force training facilities or those of other government agencies. In addition to training for AT and CT specialists, training should also be provided for potential victims of terrorism. Targets must be aware and alert if AT efforts are to succeed, and appropriate training can enhance the chances of survival of kidnap victims.

Terrorist *modus operandi* must be studied so that tactical countermeasures can be devised. Generally, terrorists have held the initiative. The barricade-and-hostage tactic has had the greatest impact, leading to the creation of special CT rescue teams around the world, including teams within the U.S. military. Each service has some type of special force for rescue operations.

Most of the AT and CT specialists' current equipment is off-the-shelf military hardware. However, there is a vast array of state-of-the-art equipment available in the private sector, including new communications equipment, ammunition and weapons, night vision equipment, and physical security devices, some of which are now finding their way into military inventories.

The future holds the threat of increasing international, state-sponsored terrorism, with nations using terrorists as "surrogate" military forces. Such forces will be able to draw on the national resources of their sponsors and thereby pose an even greater threat to the U.S. military. This trend could be significantly countered by more cross-service AT and CT initiatives. Direction and guidance for such joint efforts must come from the Department of Defense.

CONTENTS

I. INTRODUCTION

Terrorist attacks on U.S. military targets and the accompanying concern for casualties and property damage have caused the military to reevaluate its defenses against terrorism. Although military facilities and personnel are not the most frequently selected terrorist targets (U.S. diplomats have that dubious honor), some of the attacks on the military have been notable successes. The truck bombing of the U.S. Marine barracks in Beirut, which killed 241 people, was the deadliest single terrorist attack in history. The January 12, 1981, attack at Muniz Airport, Puerto Rico, in which nine A-7 aircraft were destroyed by the Macheteros, caused the greatest monetary loss (approximately $45 million).

The military's concern has also been heightened by such acts as the Red Brigade kidnapping of General James Dozier; the assassinations of military attaches in France, Greece, and El Salvador; and the attempted assassinations of Generals Alexander Haig and Frederick Kroesen.[1] These attacks, while certainly not the only ones against the U.S. military, indicate the potential of terrorism, a potential that has caused the military services to devise protective measures.

Military countermeasures can be divided into offensive, or *counterterrorism (CT)*, and defensive, or *antiterrorism (AT)*, programs.[2] Counterterrorist actions are those taken in direct response to a terrorist act. For example, actions by the military to resume control of a command post that had been assaulted and held by terrorists would

---

[1]Dozier was kidnapped on December 17, 1981, and freed by an Italian counterterrorist team on January 28, 1982. The attaches killed include Lieutenant Colonel C. R. Ray, Paris, January 18, 1982; Navy Captain George Tsantes, Athens, November 15, 1983; and Lieutenant Commander Alfred Schaufelberger, San Salvador, May 25, 1983. Terrorists attempted to kill General Haig with a road mine in Belgium on June 25, 1979; a rocket-propelled grenade was launched at General Kroesen in Heidelberg, Germany, on September 15, 1981.

[2]The Army and the Air Force have officially defined these terms as noted. The Marine Corps and the Navy apparently tacitly accept the definitions without official acknowledgment.

be labeled CT actions. Antiterrorism actions are defensive and preventive measures taken to lessen the chances of terrorist attack, such as arming the personnel of a command post, installing alarm systems, and using devices such as closed-circuit TV systems.

This Note details the current status of military AT and CT programs and illustrates some of the shortcomings in these programs, shortcomings that may be caused by a lack of cross-service cooperation and a lack of unifying service direction.

This study first details the nature of the terrorist threat to the military. Data from the Rand Chronology of International Terrorism reveal disturbing trends not only in the incidence of antimilitary terrorist attacks but in the level of attack sophistication. To offset these trends, the services are spending large amounts of money and manpower for physical protection. However, both the Congress and the General Accounting Office (GAO) have criticized the services and the Department of Defense (DOD) for a lack of control and direction in these fiscal and manpower matters. This study examines the debate. Next, the Note looks at four elements that are of specific concern to military AT and CT planners and hence are considered critical to effectively countering terrorism. The military services' specific CT and AT programs are next reviewed. The Army and the Air Force have generally been the innovators, and some of their initiatives are identified and discussed. The final section looks at the future: What is terrorism going to be like, and what, therefore, must be the services' response for self-protection? The U.S. military is a major contributor to national countermeasures efforts; to remain so, it must first protect itself.[3]

---

[3]This study is limited to internal, intraservice AT and CT efforts. The existence of a national counterterrorist capability that transcends the mission limits of the separate military programs has been noted by the media. However, discussion of a national capability is beyond the scope of the present study.

II. TERRORISM AND THE U.S. MILITARY

Terrorists seek visible, symbolic targets that hold the world's attention because of extensive media coverage. The propaganda value of such coverage is not lost on terrorists. As a superpower, the United States and its status symbols inherently have high propaganda value, and America's military installations and personnel are some of its most visible status symbols.

THE MILITARY TARGET

Data from the Rand Chronology of International Terrorism indicate that the military has become an increasingly popular target,[1] as shown in Table 1.

Table 1

TERRORIST ATTACKS AGAINST U.S. MILITARY TARGETS[a]

Time Period	Number of Attacks			
	Installations	Individuals	Random Targets	Total
1970-74	18	9	11	38
1975-79	16	7	15	38
1980-83	29	13	17	59
Total	63	29	43	135

[a]Attacks on installations and individuals are considered premeditated; random targets are targets of opportunity, and attacks against them are, by definition, not premeditated.

[1]The Chronology is derived from a variety of open sources including U.S. and foreign newspapers and magazines as well as reports of the Foreign Broadcast Information Service (FBIS). Since only open sources are used, attacks on the military that are classified are not included.

In 1980-83, there was a 35 percent increase in the number of incidents over the preceding five-year period, 1975-79 (59 vs. 38). This increase is particularly significant, since the number of incidents in 1975-79 showed no increase over the number in 1970-74 (38 in each period). The largest increase in 1980-83 was in the number of attacks against individuals (45 percent, from 7 to 13); attacks on installations increased 44 percent (from 16 to 29).

Installations are attacked more frequently because they are permanent and thus easily surveilled. Surveillance of individuals is more difficult, and they are therefore difficult to attack. In this study, installations and individuals are considered sophisticated targets, and attacks against them are considered premeditated. Premeditated attacks present greater risks for the terrorist than do random target attacks, and they involve far more forethought and planning.[2]

An upward trend in higher-order terrorist attacks is revealed when the number of premeditated actions (installations plus individuals) is compared with the total number of attacks. In 1975-79, premeditated attacks comprised 60 percent of the total incidents (23 of 38). However, in just four years, from 1980 to 1983, premeditated attacks jumped to 71 percent (42 of 59 cases). Clearly, terrorists are using more sophisticated attack modes than they have in the past. The number of terrorist acts in 1984 cannot be predicted, but it can be expected that 1984 numbers will support the conclusions that the U.S. military is increasingly popular as a terrorist target and that terrorists are getting better at what they do.

At the same time, random targets are becoming less prevalent. There was a 27 percent increase in random attacks between the 1970-74 and 1975-79 periods; there was only a 12 percent increase between 1975-79 and 1980-83.

These figures indicate that military installations and high-risk personnel should be the subjects of greatest concern in countermeasures planning, but education programs for less-than-high-risk targets are also advisable, if only to raise awareness levels.

---

[2]For example, a successful assault on a facility would require a great deal of preplanning; the firebombing of American cars parked on the street would not.

The incidence of terrorist attacks, by service, is shown in Table 2 for the period 1970-83. The Army and the Air Force, with a greater number of permanent installations than the Navy or Marines, accounted for more than two-thirds of the 77 incidents (53, or 68.8 percent). The Army and the Air Force employ about 65 percent of the personnel in the four services; thus there is a high correlation between number of people and number of terrorist incidents. While the Navy has more personnel than the Air Air Force, it has fewer shore installations and has suffered less terrorism. The Marines, being the smallest service, have had the fewest incidents, although the Beirut attack on the Marine headquarters produced the largest number of casualties of any single attack.

To summarize:

- Terrorist attacks on U.S. military targets are increasing.
- There has been significantly more antimilitary terrorism in the 1980s than at any time in the past.

Table 2

NUMBER OF TERRORIST INCIDENTS IN 1970-83, BY MILITARY SERVICE

Military Service	No. of Incidents[a]	Percent of Total
Army	27	35.1
Air Force	26	33.8
Navy	17	22.1
Marines	7	9.0
Total	77	100.0

[a]Of the 135 incidents listed in Table 1, only 77 were identifiable by service.

- Terrorist attacks requiring a higher degree of sophistication are on the rise.
- Attacks on random targets are increasing more slowly than attacks on installations or individuals.
- The Army and the Air Force, having more installations and personnel, will probably continue to receive the greater share of terrorist action.

COSTS FOR SECURITY

Thus far, only a limited effort has been made to determine the military's security costs. In 1981, a GAO report on military physical security criticized the DOD for its lack of an organized security management system:

> Normal management system elements--providing guidance and criteria, assuring proper implementation, and monitoring--do not exist within Defense or among the services except to a limited degree for certain highly sensitive assets [nuclear and chemical weapons and materials; arms, ammunition, and explosives; and classified information].[3]

The GAO estimated military physical security costs at about $2 billion annually--approximately $1.8 billion for personnel expenses, the balance for equipment, R&D, and security upgrade programs. Although not considered totally accurate by the GAO, these costs nevertheless provide a yardstick by which to measure the services' physical security programs. Following the GAO report, the House Investigations Subcommittee of the Armed Forces Committee held a hearing during which the DOD furnished strength figures for military physical security personnel for each of the services.[4] These figures are given in Table 3, which shows that there is an inverse ratio between the size of the

---

[3] *Defense Needs Better System for Assuring Adequate Security at Reasonable Cost on U.S. Bases,* General Accounting Office, Report to The Congress, PLRD-81-1, March 6, 1981, p. 24.

[4] U.S. Congress, House, Investigations Subcommittee of Committee on Armed Services, *Hearing: Physical Security at U.S. Military Bases,* 97th Cong., 1st Sess., July 17, 1981.

Table 3

MILITARY PHYSICAL SECURITY PERSONNEL, BY SERVICE

Service	Total Force[a]	Number of Security Personnel	Percent in Security
Army	1,131,413	8,774	0.8
Navy	822,162	11,991	1.5
Air Force	793,714	27,928	3.5
Marines	206,930	11,725	5.7
TOTAL	2,954,219	60,418	2.0

[a]The total force figures include active-duty military and civilian personnel. These personnel levels are for 1981, the year of the GAO report and the Congressional hearing. Active-duty military levels were obtained from *The Budget of the United States Government, Fiscal Year 1980*. Civilian strength figures for the Army, Navy, and Air Force were obtained from the *Statistical Abstract of the United States, 1980*. Marine Corps civilian strengths were estimated from information provided in Department of the Navy sources.

service and the percentage of the force assigned to security duties.[5] The smallest service (the Marines) has the highest percentage of its troops assigned to security duties. While there is no magic formula for determining the appropriate number of security personnel for each service or for determining the percentage of the total force that should be assigned to security duties, the increase in terrorism in recent years indicates that the current percentages may have to be revised upward for all four services.

[5]Congress questioned the reliability of the security personnel figures, since they include only full-time personnel; part-time personnel were not included by the services. See U.S. Congress, House, Investigations Subcommittee of the Committee on Armed Services, *Report: Physical Security at U.S. Military Bases*, 97th Cong., 1st Sess., November 5, 1981, p. 7.

Equally significant are the cost figures shown in Table 4.[6] Like the personnel figures in Table 3, they show an inverse relationship between the size of service and the amount spent per member for physical security personnel. The figures in Table 4, like those in Table 3, may be somewhat inaccurate, but the difference between the Army's $101.70 per member and the Marines' $1033.90 per member is dramatic. The fact that the Marines may be spending over $1000 per person for physical security, while the Army is spending less than 10 percent of that amount points, at a minimum, to the need for further research into actual costs for physical security.

As a major DOD budget item ($2 billion annually), physical security is like personal security, an area for which there is no accurate system to measure dollar or manpower costs. All that is available are the suspect figures developed by the GAO and questioned by the Congress. The GAO recommended that physical security costs become a "line item" in military budget forecasts, but the services have apparently not yet taken this step.

Table 4

MILITARY PHYSICAL SECURITY COSTS

Service	Costs[a] ($ millions)	Security Cost per Member[b] ($)
Army	115	101.7
Navy	195	237.2
Air Force	369	465.3
Marines	213	1033.9
Total	892	301.9

[a]Costs are for personnel only and do not include equipment or R&D.

[b]Determined by dividing total-force figures from Table 2 into costs.

[6]Cost figures derived from U.S. Congress, House, *Hearing*, p. 37, and U.S. Congress, House, *Report*, p. 7.

To summarize:

- The four services are spending at least $2 billion annually on physical security.
- There is currently no accurate accounting of these security costs.
- The most frequently attacked services assign fewer personnel to security duties and spend less for security per person than do the less frequently attacked services.
- As the incidence of antimilitary terrorism goes up, the percentage of personnel assigned to security duties may have to rise.

The increase in terrorist attacks on the military services may be due to the recent escalation of state-sponsored terrorism.[7] State-sponsored terrorist groups, with their sponsors' manpower, financial, logistics, and intelligence resources, constitute a significantly greater threat than do nonsponsored groups. As certain nations increase their use of terrorist "surrogates" to project national goals, the U.S. military will most likely remain an increasingly popular target. Its symbolic target value will not diminish over time; in fact, it may increase, particularly if America maintains its hard-nosed stance on international terrorism. America has thrown down a figurative gauntlet, and international terrorists have picked it up. Like other symbolic U.S. targets (e.g., diplomats and multinational corporations), the military services should prepare for increasingly sophisticated and bloody terrorist actions. These preparations will most likely absorb an increasingly greater percentage of military budgets, but in view of the seriousness of the threat, such costs will have to be accepted. Accurate accounting of physical security outlays (as called for by the GAO) therefore seems not only reasonable, but mandatory. While possibly not as advanced as other technologies, the technology for infantry-style small arms and physical security devices is improving. More efficient budget control should yield a truer picture of AT and CT asset costs. With these controls and identification processes, the funds that are allocated can be more wisely and efficiently spent.

---

[7]See Brian Michael Jenkins, *New Modes of Conflict,* The Rand Corporation, R-3009-DNA, June 1983, pp. 12-13.

III. COMPONENT ELEMENTS

The critical elements of effective and efficient AT and CT programs are

- Credible, reliable, and timely intelligence.
- Education and training.
- Modern tactics and techniques.
- Up-to-date equipment and devices.

Effective use of each element can reduce the vulnerability of targets (both persons and facilities) and lessen terrorism's impact. Failure to attend to any one of them could increase the potential for terrorist targeting. As the effectiveness of each element increases or decreases, so will that of the others. Thus, for example, an effective intelligence system has a direct bearing on education and training programs; if intelligence information is outdated, so will be the programs that teach its lessons.

INTELLIGENCE REQUIREMENTS

Timely intelligence information about terrorist activities is of primary importance to AT and CT efforts, yet gathering, analyzing, and disseminating information about clandestine organizations--often very small, compartmented cells--is extremely difficult. Adding to the difficulty is the increasingly effective use of "tradecraft," or sophisticated organizational techniques, by terrorists.[1] In the early days of urban political terrorism (prior to the mid-1970s), terrorists employed relatively poor security practices. However, with training in Middle Eastern camps, terrorists became more aware of security.

---

[1]The increase in terrorist tradecraft effectiveness has been noted, for example, by Paul Johnson, "The Seven Deadly Sins of Terrorism," *NATO Review*, Vol. 28, No. 5, October 1980, pp. 28-33. Johnson says, "... and, not least, the organizational techniques with which these weapons and skills are deployed [by terrorists] are all improving at a fast and accelerating rate" (p. 30).

Although the intelligence community's capabilities have increased over the years, the concurrent increases in the terrorist's security awareness have negated some of these advances.

The collection and use of intelligence information on terrorists have been plagued by two significant problems. The first arose in response to criticism of domestic intelligence operations during the Vietnam War and post-Watergate eras, which led to severe constraints on U.S. intelligence collection and information retention. Questionable practices by military and civilian intelligence organizations in the 1960s led to some programs being seriously cut back, in some cases to the point of virtual nonexistence.[2] Legal, legislative, and administrative constraints (along with leaks of both sensitive information and identities of sources) seriously undermined U.S. intelligence collection programs and relationships with foreign counterpart agencies. Foreign intelligence programs were affected as well. The Reagan Administration, however, has taken initiatives to reverse this trend, and a more lively intelligence apparatus seems to be forming.

In 1980, one of the high-priority targets of both the CIA and friendly intelligence services was the penetration of the terrorist organizations functioning on the world stage.[3] There appears to be an emerging consensus that the nation must be provided with a functional, efficient intelligence apparatus--one that operates within legal bounds.[4] It is unfortunate that terrorist successes against military

---

[2]See Sorrel Wildhorn, Brian Michael Jenkins, and Marvin M. Lavin, *Intelligence Constraints of the 1970s and Domestic Terrorism: Vol. I, Effects on the Incidence, Investigation, and Prosecution of Terrorist Activity*, The Rand Corporation, N-1901-DOJ, December 1982; and Marvin M. Lavin, *Intelligence Constraints of the 1970s and Domestic Terrorism: Vol. II, A Survey of Legal, Legislative, and Administrative Constraints*, The Rand Corporation, N-1902-DOJ, December 1982.

[3]Cord Meyer, "The Collectors," *Intelligence Requirements for the 1980's: Clandestine Collection,* National Strategy Information Center, Inc., 1982, p. 218.

[4]One effect of Congressionally directed curtailments on AT and CT operators was the erasure of potentially vital threat information. Destruction of files and databanks prevented military intelligence agencies from keeping decisionmakers informed about potentially threatening terrorist groups. Not only were files and databanks destroyed, but military collectors were prevented from utilizing previously productive nonmilitary sources of information.

targets had to provide some of the impetus for a more reasoned approach to military intelligence efforts.

The second problem is an internal one, involving the institutional prejudices of the intelligence function, on one side, and the operations element, on the other. When looking to place blame for a failed mission, the operations element says, "The intelligence people never told us." Conversely, the intelligence specialist says, "Ops never asked us, and we cannot guess what they want." This lack of coordination, called the "Green Door syndrome," has been cited as one of the reasons for the failures in the Son Tay and Iranian rescue missions.

The Green Door syndrome has probably plagued military planners as long as military operations have existed, and its effects can be critical. Indeed, national security (and prestige) can depend on whether the "door" is opened or closed. The proper exchange of needs and requirements between operators and intelligence personnel can spell the difference between life and death in the field, or the success or failure of a mission. The solution to the Green Door is not simple, but a way must be found for operations and intelligence to interact with each other continually. One potential solution might be the assignment of operations and intelligence personnel in the same function, thereby lowering some of the barriers to effective communication. The Long Commission Report on the bombing of the U.S. Marine headquarters in Beirut recommended the creation of an all-source information center.[5] Such a center should have permanent assignments of operations personnel.

The intelligence needs of the AT and CT regimes differ. The CT requirements are perhaps more tactically oriented than those of AT. The CT force responding to a barricade-and-hostage situation needs to know where the terrorists are located, how they are armed, how many hostages there are, how the building is designed and constructed, and similar situation-specific information.[6]

---

[5] *Report of the DOD Commission on Beirut International Airport Terrorist Act, October 23, 1983,* December 20, 1983.

[6] See Howard R. Simpson, "Organizing for Counter-Terrorism," *Strategic Review*, Winter 1982, pp. 28-33.

Whereas the CT operator needs specific data, the AT specialist needs dynamic information that enables him to increase or decrease his defensive systems as threats change. The AT element cannot protect all prospective targets equally, nor can any target be protected well enough to guarantee it immunity from terrorism. Robert Moss, a London-based terrorism expert, appearing before the Senate Subcommittee on Security and Terrorism in 1981, testified:

> You cannot protect every target. You cannot protect every installation. You can do something about the most obvious and the most important. You cannot imagine for a moment that if your society faces a concerted terrorist campaign that you can mount static defense for every likely target.[7]

The best the AT operator can hope for is that his efforts will cause terrorists to judge potential targets as too costly to attack. He looks for indicators of future terrorist action such as discovered arms caches, travel of known or suspected terrorists across borders, and targeting patterns noted in other countries. Analysis of these indicators may help predict the sites of upcoming terrorist activity, and security at those sites can be increased.

EDUCATION AND TRAINING

The three primary "students" of the terrorist threat are the CT specialist, the AT specialist, and the potential victim or high-risk individual.[8] Each needs to know his enemy; accordingly, countermeasures education should be designed with that goal in mind. The purpose of this education is not to overestimate the terrorist's capabilities, but to objectively evaluate the threat. As terrorists change their methods, students need to be informed so that they can make adjustments in countermeasures programs; consequently, refresher courses may be useful adjuncts to awareness programs.

---

[7] *Terrorism: The Role of Moscow and Its Subcontractors*, Hearing Before the Subcommittee on Security and Terrorism, 97th Cong., June 26, 1981.

[8] For purposes of this study, education is defined as the learning of concepts or ideas; training is defined as the acquisition of skills.

The CT specialist's education should be aimed at understanding the psychology of terrorism and terrorists, including the so-called "terrorist mindset." The ability to think like a terrorist is vital to the CT operative, who must

> have insight into terrorist psychology and some idea of terrorist strengths and weaknesses.... Every move of a counter-terrorist unit, particularly the ultimate decision to use lethal force, must be based on the best knowledge available of the terrorists' motivation and probable reaction. This requires the application of above-average intelligence in addition to finely honed combat skills.[9]

The AT operator also needs an education program that will help him anticipate terrorist actions. Such a program, using terrorist history as a foundation, augmented by current trends, can give both the CT and the AT specialist a well-rounded understanding of the adversary.

An effective AT program also requires that potential victims be aware, alert, and cooperative. Being alert and aware means having an objective appreciation of the threat so that appropriate precautions can be implemented to reduce vulnerability. The potential target can be an individual, a military base, or any facility that appears vulnerable to terrorist attack. High rank is not the only criterion defining high-risk individuals. Military personnel of relatively low rank assigned to high-threat areas may also qualify for countermeasures protection. Also, certain positions or assignments are, by their symbolic nature, attractive terrorist targets, e.g., military advisors, military attaches. These high-risk targets must be educated and made aware of terrorism's dangers.

Educational programs on military installations or other facilities may become unwieldy due to the number of potential students. But many of the people at these sites can be given limited information about terrorism that is sufficient to alert them to suspicious activity.

The crisis or threat-management staffs at these installations must also be educated about terrorism. If these groups do not understand terrorism, they will be unable to operate effectively in times of

---

[9]Simpson, op. cit., pp. 30, 31.

terrorist-inspired crisis. The crisis-management staff should also perform realistic exercises so that they can evaluate countermeasures plans and test various options for effectiveness. The time to train a crisis management staff is *before* an actual incident, not *during* one.[10] This is as true for the CT operator as it is for the crisis manager.

CT training must be rigorous and continual. Peak physical conditioning is necessary, as are marksmanship and the other skills of qualified commando or Special Weapons and Tactics (SWAT) team members. These qualifications are outlined in a recent *Military Technology* article, which observed that CT team members must be physically and psychologically prepared to stand up to "critical stress situations."[11] Their training must be "all-encompassing," with emphasis on marksmanship, close-in combat, tactics, climbing, etc. Other skills include silent movement and communications techniques; building penetration; search and clear techniques; team coordination and interaction; and use of team weapons. The critical need to maintain peak proficiency has led to some problems of "burnout" in team members who get to use their skills only in practice, never in real situations.[12]

AT training, like CT training, must reflect the unique needs of the job. Special AT skills include proper techniques for protecting threatened individuals, such as methods of moving potential victims from one location to another. Of course, not all AT specialists are bodyguards. Some are experts in physical security methods, who must have special skills to ensure that physical security standards match the

---

[10]In Simpson's words, "The best minds, the best equipment, the best preparation and the best possible decision may not avert disaster. Countering terrorism is a question of meeting a fluid crisis situation with as many odds as possible in your favor." (Op. cit, p. 29.)

[11]Karl Gerhard Bornmann, "Modern Weapons and Equipment Increase the Striking Power of Counterterrorist Groups," *Military Technology*, August 1982, pp. 155-160. Bornmann is a weapons and equipment expert with the West German Federal Border Guard.

[12]The "burnout" problem may not affect civilian (police) SWAT teams as much as military teams, because civilian units have more exposure to real crisis situations. Hostage situations are rare in the military.

threat at a given time and place; others are specialists in defensive driving who are trained to evade terrorist vehicular operations (such as roadblock kidnappings or assassinations).

Specialized training is also available for high-risk individuals, for example, in marksmanship and familiarity with weapons. Hostage survival training should be provided for certain individuals, while others may need defensive driving training.

It is essential that security personnel be familiar with firearms--unfamiliarity can be fatal. During the kidnapping of the OPEC oil ministers in Vienna in December 1975, an Austrian policeman attempted to shoot it out with Carlos, the terrorist leader. The policeman tried to use a submachinegun with which he was unfamiliar; he was unsuccessful, and Carlos killed him.

Hostage survival training may be presented in the classroom or combined with training exercises. Former hostages and POWs with even limited exposure to hostage survival techniques have reported that the knowledge they did have helped them survive. Thus, while a combination of classroom education and field practice may be an ideal learning situation, it may not be necessary for all potential hostages.

TACTICS AND TECHNIQUES

The concept of countermeasures tactics to be taught in educational programs and implemented in training programs should reflect current analysis of intelligence about terrorist *modus operandi*. As terrorists' methods change, so must the countermoves.[13] The CT tactics needed to assault a multistory building are different from those required to attack an offshore oil platform or a parked aircraft. From the AT standpoint, as methods of terrorist attack change (e.g., using suicidal truck bombers rather than unoccupied car bombs), physical security techniques must be adjusted. In the case of suicide truck drivers, new roadblock devices may have to be designed.

---

[13]See Bornmann, op. cit., p. 155.

Historically, the initiative has mostly been with the terrorists. As their techniques have changed, CT and AT forces have had to adjust.[14] When transnational terrorists began hijacking aircraft in 1968, governments began designing counterhijacking techniques, such as the use of skymarshals and the creation of CT teams, including the West German GSG-9, which was so successful at Mogadishu, Somalia. Hijackings also prompted the ever-present AT airport security screening procedures familiar to all travelers. As letter bombs became popular with terrorists, revised mail screening methods were implemented, and new electronic devices for spotting mailed explosives came on the market. Explosives-sniffing dogs were trained and are now part of many military and civilian police K-9 sections. As vehicular kidnappings and assassinations became popular tactics, potential victims and the AT community became increasingly interested in defensive driving and armored cars.

The terrorist assault tactic with possibly the greatest impact on countermeasures development has been the barricade-and-hostage situation. Aircraft hijackings, embassy takeovers, and other operations that led to the taking of hostages have caused governments to organize special rescue teams. In fact, "the rescue operation has now become a distinct type of military undertaking, on a par with commando raids, long-range reconnaissance and irregular operations."[15]

It would be erroneous, however, to assume that CT and AT planners are without foresight when it comes to implementing changes. Nuclear terrorism is a case in point. Although there has never been a terrorist assault on U.S. military nuclear weapons, either in transit or in storage, those charged with nuclear security have made significant improvements in systems designed to thwart small-unit attacks. New alarm and defensive systems have been installed in and around storage areas. New high-security transport systems have been designed to move nuclear weapons. These innovations may, in fact, be responsible for the paucity of terrorist attacks against military nuclear weapons. Their

---

[14]See Johnson, op. cit., p. 33.

[15]Bruce P. Schoch, "Four Rules for a Successful Rescue, *Army*, February 1981, p. 22.

effectiveness, however, can only be demonstrated if terrorists should try to assault special-weapons targets.

Another example of a countermeasure that may have preempted terrorist acts is an Air Force education program that teaches personal security tactics and techniques to selected military people before assignment to high-threat environments. The students, many with little or no prior knowledge of terrorism, have been taught basic security awareness--the principles of staying alert, not being predictable, keeping a low profile, proper use of weapons, travel/vehicle security, and cultural dos and don'ts. The training has resulted in increases in reports of suspicious activity, e.g., possible preoperational surveillance, against military personnel and facilities. Awareness may not always preclude terrorist attack, but evidence has shown that many attacks against military personnel were not carried out because the personnel were "very security-conscious."

EQUIPMENT AND DEVICES

Some equipment presently used by CT and AT personnel (e.g., M-16 rifles, handguns, shotguns, submachineguns, armored vests and flak-jackets, communications equipment, and night vision equipment) was originally intended for more standard military functions. Many kinds of equipment and devices have, of course, been developed for the specific purpose of fighting terrorism (e.g., airport screening devices and mail screening equipment).[16]

To successfully complete his mission of saving lives and restoring normal order and discipline, the CT specialist needs good, reliable equipment. Bornmann noted, "One of the main problems facing [CT forces] is to approach violent persons unnoticed, in order to put them out of action as quickly as possible. Essentially this is a tactical problem, but technical support is ... necessary."[17] New equipment is continually being developed. Improved small arms, grenades, clothing, and specialty items such as ladders coated with soundproofing material

---

[16]Bornmann, op. cit., p. 160. Bornmann also reports that industry has recognized the special needs of countermeasures forces and has responded accordingly.

[17]Ibid., p. 158.

are coming on the market. Smaller, more reliable, and more secure radio equipment is constantly under development. Communications security has been enhanced by the use of scrambler technology in small, hand-held radios. Terrorists in the past have eluded capture by monitoring police radio frequencies. Through the use of special band-switching (frequency-changing), scrambler-capable radios, police operations have become more secure and therefore more successful.

The ability to clandestinely infiltrate and exfiltrate an area is also improving. Stealth techniques, recently in the news in connection with the Air Force's bomber force of the future, can be applied to the tactical CT role as well.[18] This technology becomes increasingly important as terrorists learn the methods used by counterterrorist forces and develop their own counter-countermeasures. This leap-frog effect is likely to continue, especially as state-sponsored terrorism becomes more prevalent and terrorists can draw on their sponsors' technology.

Lightweight, concealable body armor is a relatively new development for both civilian and military users. Vests can now stop regular handgun ammunition and possibly some lightweight rifle bullets. However, the future utility of vests may be compromised by the advent of several new varieties of very powerful handgun ammunition. These bullets will penetrate so many layers of Kevlar (the Dupont material from which most soft body armor is made) that effective vests would be impractically bulky. Equally disquieting is the presumption in many foreign countries (e.g., Turkey) that Americans are so rich that they all wear bulletproof vests. Assassins, therefore, have begun aiming for the head and not the chest or back (presumably the protected areas) of their American victims. An additional shortcoming of armored vests was dramatically demonstrated when John Hinckley tried to assassinate President Reagan: Although the President was wearing a vest, he was struck in an unprotected area under his arm.

---

[18]The commercial movie production "Blue Thunder" contained a credit line indicating that silent helicopter flight and other capabilities are real and available.

New developments in special ammunition can benefit security personnel as well as terrorists. A new type of bullet developed by a French munitions manufacturer and called the THV is designed for abrupt deceleration in "soft targets."[19] The implication is that all of the bullet's energy is expended quickly in a human body and will not exit the body to become a ricochet dangerous to innocent bystanders. This is an important capability for CT and AT personnel concerned with innocent people being injured in assault crossfire. The high relative stopping power (RSP) of these bullets means the terrorist immediately ceases to be a threat to nearby persons.[20] A British ammunition equal to or even more devastating than the French bullet has also been reported.[21] And these are only two of many such developments. Of course, if this ammunition finds its way into terrorists' hands, the results could be fatal for AT and CT forces as well as the citizens they are charged with protecting. This concern has not been missed by critics of advanced ammunition who point to the attempt on President Reagan's life in which the would-be assassin used special .22 caliber ammunition.[22]

Equally impressive changes have been made in small arms. Both the West Germans and the Israelis have developed new, smaller and more concealable submachineguns. The West German effort may have been partially the result of the experience of GSG-9 at Mogadishu. Working in confined quarters, such as an aircraft cabin, dictates the use of small, maneuverable weapons. At Mogadishu, GSG-9 used longer, less-maneuverable submachineguns than are now available. The Israelis have

---

[19]"Very-high-velocity Small-arms Ammunition," *International Defense Review*, No. 10, 1983, p. 1471.

[20]RSP is defined as the relative ability of a shot to render an adversary instantly incapable of further aggression. See William J. Bruchey, Jr., *Ammunition for Law Enforcements: Part I, Methodology for Evaluating Relative Stopping Power, and Results*, Ballistic Research Laboratory, Aberdeen Proving Ground, Technical Report ARBRL-TR-02199, October 1979.

[21]*International Defense Review*, op. cit., p. 1506.

[22]The bullets, called Devastators, were explosive-tipped and were supposed to explode on impact. However, the one that hit President Reagan did not. See *Time*, April 13, 1981, p. 29.

begun manufacture of a mini-Uzi submachinegun (the Uzi is one of the most common submachineguns in the world). The same weapon characteristics favorable to CT elements are needed by AT personnel working inside cars when protecting high-risk individuals. In addition to shortened submachineguns, cut-down shotguns have also been developed, several of which have foldable stocks and shortened barrels.

Night vision devices are in their second or third generation, after being widely used by guards in Southeast Asia patrolling nighttime perimeters. More advanced nighttime devices employ laser technology, e.g., laser gunsights which, once zeroed for accuracy, enable a marksman to hit the exact spot on which an illuminated laser dot is projected. As a recent report noted, for those who are aware of the technology, "the appearance of a spot of light on a potential target could have an intimidating effect, which could prevent shooting and a subsequent escalation of violence."[23]

Equipment for enhancing physical security at protected sites and installations--alarm systems, intrusion detection devices, response force operations, fencing, and locks--is needed by the AT specialist, although it is of little use to CT. The AT operator needs to know the advantages and limitations of his physical security screening devices. The false sense of security provided by seemingly impenetrable barriers disappears quickly during an attack by dedicated intruders. In research performed for the Army, it was noted that

> Barrier penetration data ... can be reasonably interpreted to show that the most effective of the current perimeter fencing configurations now in use at [nuclear weapons storage sites] can easily be penetrated by motivated intruders in less than 30 seconds.... the probability that response forces can deploy rapidly enough to prevent penetration of the perimeter seems very low.... The National Bureau of Standards ... has concluded that perimeter fencing of the sorts and configurations in present use, will not, by its hostile appearance, deter terrorists.[24]

---

[23]"LASIII Laser Aiming Point," *International Defense Review*, No. 10, 1983, p. 1471

[24]*An Evaluation of Perimeter Barriers and Lighting Effectiveness*, U.S. Army Mobility Equipment Research and Development Command, Final Report, June 1, 1979, pp. II-13-14.

Continued research into physical security barrier technology is needed, as is research in other disciplines that affect AT and CT specialists.

There are various types of technology-intensive devices that come with very high price tags, but since military budgets are limited, availability does not imply possession. At certain locations, however, state-of-the-art equipment may be essential to deal with the terrorist threat. Selecting the locations with the most critical needs is a difficult job that each military service will have to do for itself. Military departments must decide where best to position their limited countermeasures equipment on the basis of available intelligence information and the level of education and training of their tactically skilled personnel. How these limited resources are used will at least partially determine the effectiveness of the intelligence system.

The interrelationship between the four critical elements of an effective AT/CT program has already been mentioned. With good, sound intelligence, education and training programs can be tailored to fit the threat. Educated and trained AT or CT specialists, along with the individuals who are potential targets, can develop the tactics and techniques best suited for expected assaults. As terrorist tactics change, industry (working in concert with both AT and CT elements) can manufacture the equipment and devices needed to meet evolving challenges.

As might be expected, with each service having its own distinct CT and AT programs, those programs vary. There are several areas in which the services could benefit from interservice cooperation. In some cases, such cooperation is already under way. Other potentially beneficial areas for joint consideration are highlighted in the next section.

IV. THE MILITARY SYSTEMS

CT PROGRAMS

The Army and the Air Force have been the major innovators in developing internal counterterrorist doctrine, plans, organizations, and response capabilities. This may be due, at least in part, to their respective situations in Vietnam, where both had more vulnerable installations that were difficult to protect from insurgent attacks than did either the Navy or the Marines. Such attacks included small-unit infiltrations, standoff mortar and rocket barrages, and large-unit assaults (such as the major assaults that occurred during the Tet Offensive in January-February 1968).

As a result of this concentrated exposure to insurgency, the Army and the Air Force developed protective and reactive systems unique in their military histories. The Air Force had to create innovative physical security devices, intelligence-gathering systems for early warning of insurgent attack, and small-unit response capabilities to counter the new challenge of defending its perimeters against a unique and resourceful foe. (The Army, with its conventional ground (infantry) role, was already acquainted with this requirement.) The innovative thinking engendered by the nature of the threat, the lack of assistance from ground-oriented services, and the lack of Air Force experience in defense against insurgency has continued into current Army and Air Force countermeasures initiatives against political terrorism.

At about the same time the Army and the Air Force were learning to cope with insurgent attacks against their Southeast Asian bases (the mid-1960s), U.S. law-enforcement agencies were developing the first SWAT teams, whose function was "to terminate armed confrontations with minimum use of force."[1] The civilian SWAT team was the foundation for the military services' current counterterrorist response capability: Military teams are modeled after their civilian police counterparts.[2] For example, the Air Force SWAT unit (called an Emergency Service Team,

---

[1]Gerald W. Boyd, "Special Weapons and Tactics Teams: A Systems Approach," *FBI Law Enforcement Bulletin*, September 1977, pp. 21-26.

[2]These teams also have functional uses in nonterrorist threat

or EST) is a four-man team composed of a team captain, a marksman, a point man or guide, and a defense man.[3] The Army's Special Reaction Team (SRT) has the same basic structure as the Air Force EST, but it includes a fifth team member, an observer.[4]

These special teams are trained to evacuate innocent bystanders, rescue hostages, apprehend perpetrators, use riot-control agents (e.g., tear gas) and small arms, provide selective firepower (e.g., snipers), and surreptitiously enter buildings or locations via climbing or rappelling techniques.[5] Normally they are made up of volunteers from the services' military police organizations. Each service has its own methods of training these special teams. Air Force EST leaders are sent to a special Air Force course where they undergo an intensive two-week curriculum that prepares them to train their own team members when they return home. Marine Corps members receive their training from the Federal Bureau of Investigation at the FBI Academy at Quantico, Virginia.

The military's CT capability is not limited to SWAT units. Some installations and facilities also have infantry-style (large-unit) forces that can be used in emergencies. Moreover, SWAT teams may, in some cases, be inappropriate as a response force. For example, USAF policy for regaining control of Air Force nuclear assets in unauthorized hands states that all necessary force will be applied to regain immediate control of the device(s). This policy is not altered if

---

situations such as barricade-and-hostage or sniper scenarios caused by criminals or the emotionally distraught--situations that are more likely to occur than terrorist action on military bases.

[3]"Emergency Service Teams-Hq USAF," *TIG Brief*, May 16, 1983, p. 3. The first Air Force ESTs, formed in April 1977, were to be used only on U.S. Air Force bases and only as a last resort.

[4]*Countering Terrorism on US Army Installations*, U.S. Army Training Circular TC 19-16, April 25, 1983, p. 9-11.

[5]Schoch, op. cit., pp. 22-24, outlines four principles of rescue operations: "1. The objective is to liberate, without further harm, as many hostages or prisoners as possible, without acceding to the unacceptable hostile demands. 2. The size and armament of the force must be the minimum essential to secure the release of the hostages and to neutralize the immediate hostile threat. 3. Rescuers must make the maximum possible use of all available intelligence resources to learn everything possible about the enemy, the hostages, and the target. 4. The rescue force must be a professional, integrated team that conducts operations deliberately, intelligently and with due consideration to speed, coordination and the unique nature of the mission."

hostages have been taken: The use of deadly force is authorized in any case. As currently constituted, Air Force ESTs do not have the firepower for this mission and would therefore not necessarily be called upon to respond to nuclear emergencies.[6]

Under certain circumstances, military CT response teams may be limited to picket duty. Most military installations in the Continental United States (CONUS) are on federal property and therefore fall under the investigative purview of the FBI. As the Army has stated:

> The FBI must be notified immediately [in the event of a terrorist incident on a military installation]. They will assume jurisdiction if it is determined that the incident is a matter of significant federal interest.[7]

At overseas locations, various Status of Forces Agreements and Memorandums of Understanding with host governments dictate military commanders' options for responding to terrorism on their bases. The commanders must also coordinate these matters with the Department of State and the U.S. embassy, both of which may play a key role in any terrorist incident at an overseas U.S. military base.

The Lead Agency rule, wherein the agency with prime jurisdiction takes command of the situation, applies both overseas and in the CONUS. For example, in a nonmilitary CONUS incident such as an aircraft hijacking, the key agencies are the FBI and the Federal Aviation Administration (FAA). If the hijacked aircraft is in-flight (which includes sitting on the airport ramp with the doors closed), the FAA has jurisdiction. If the aircraft is not in-flight (i.e., is on the ramp with the doors open), the FBI is the key agency. The same principle applies to the military as well in some circumstances; the military may have to stand aside for the FBI, the FAA, the State Department, etc. A variety of Memorandums of Understanding have been written to eliminate

---

[6]The USAF has special Security Police units (Quick Reaction Teams (QRT)) for nuclear response. A QRT, composed of 15 persons, can respond to the scene of a nuclear incident within 5 minutes. Potentially, EST members could have some psychological barriers to completing a mission where hostages' lives are of secondary importance, since their training emphasizes saving lives.

[7]Training Circular TC 19-16, op. cit., p. 8-3.

some potential jurisdictional problems. Nevertheless, the military commander never abrogates his

> authority and responsibility to take actions necessary to maintain good order and security on his or her installation. *This includes the initial response to an on-post terrorist incident....* If the FBI declines to exercise its jurisdiction, deciding the incident is not of significant federal interest, *the military will take action to resolve the incident.* Under either circumstance, it is incumbent upon the installation commander to take *immediate action* to prevent loss of life and/or reduce property damage prior to the arrival of the FBI response force [in a CONUS incident].[8]

AT PROGRAMS

The military's AT programs tend to follow the same pattern as its CT programs: The Army and the Air Force developed the models for the AT intelligence systems, the education and training curricula, and the testing and procurement of equipment and devices. Again, history may explain this phenomenon. As previously noted, the Army and the Air Force were the victims in 68 percent of the identifiable incidents between 1970 and 1983 (see Table 2). Being more susceptible to terrorist attack (by virtue of having both more installations and more personnel), the Army and the Air Force are more likely to be targeted by a greater variety and number of terrorist groups. Therefore, they have enhanced their AT efforts more than the Navy or the Marines.

One early intelligence program was begun by the Air Force Office of Special Investigations (AFOSI),[9] which saw a need for intelligence on political terrorism. In the early 1970s, AFOSI was publishing more than 90 percent of all U.S. government intelligence about political terrorism. Due to new programs begun by the other services and some government agencies, that percentage has fallen, although AFOSI still publishes a wide variety of intelligence products ranging from Intelligence Information Reports (IIRs) containing raw, unprocessed information from field agents to Special Reports--in-depth analyses of long-term counterintelligence problems.[10] The AFOSI counterintelligence

---

[8]Ibid., pp. 8-3, 8-4.

[9]AFOSI conducts the criminal, counterintelligence, and procurement/contract fraud investigations for the Air Force.

[10]For a complete listing of AFOSI's periodic counterintelligence

function manages both information collection and analysis and also oversees other AFOSI antiterrorist programs. These include units permanently assigned in Europe to protect selected senior officers, specialized vulnerability surveys at locations throughout Europe and the Middle East, personal briefings to general officers traveling to high-threat areas, and courses in defensive driving for both senior officers and their drivers.

While AFOSI is a major contributor to the total Air Force AT effort, overall policy, direction, and guidance for the program comes from the Office of Antiterrorism (IGT), which is also assigned to the Inspector General. Air Force Regulation 208-1 documents IGT's charter to oversee the Air Force's AT program as

> A coherent series of plans, policies, and procedures that is designed to reduce the vulnerability of US Air Force personnel and resources to terrorist attacks. It includes security precautions, defensive measures, and hostage survival training, all designed to cope with the terrorist threat.[11]

The Security Police are assigned responsibility for physical security, resource protection, information security, and installation security for the Air Force. As already noted, they also furnish the Air Force's CT response capability. AFOSI's primary contribution is in AT, but with its worldwide collection and reporting systems, it serves the CT community as a source and conduit for intelligence information about terrorists.

The Army has a somewhat different approach to its AT and CT programs. Although it defines the two terms the same as the Air Force does, the Army makes no distinct separation between the two functions and uses a consolidated organization to centralize its AT/CT roles. The doctrine, policy, and guidance functions are all located in a Terrorism Counteraction Office at the Army Command and General Staff College, Fort Leavenworth, Kansas. The Air Force AT element is centered in Washington, D.C., while its CT structure is basically guided by the Security Police, headquartered at Kirtland AFB, New Mexico.

---

reports, see "AFOSI's Counterintelligence Program: Tailor Made," *TIG Brief*, November 29, 1982, pp. 1-2.

[11]AFR 208-1, *The US Air Force Antiterrorism Program,* October 23, 1982.

The major Army intelligence organization for terrorism information is the Intelligence Threat Analysis Center (ITAC), an organization assigned to the Army's Intelligence and Security Command. The Army's willingness to budget for improvements in its terrorism reporting capability has paid dividends in ITAC's reputation in the counter-measures arena. ITAC publishes monthly intelligence summaries and threat analyses on request. Other Army intelligence sources include the Army's Provost Marshal (Military Police) system and the Criminal Investigation Division (CID).[12] These offices maintain contact with outside (civilian) agencies that collect information about potential terrorist activity.

The Navy's intelligence operations are handled by the Office of Naval Intelligence and the Naval Investigative Service. The Marines, through their counterintelligence and Provost Marshal functions, receive information from and interface with the intelligence community. Marine counterintelligence teams assigned to the Fleet Marine Force provide information and education for seagoing Marines. On occasion, the Marines have called on Army support, in the form of Mobile Training Teams, for information about terrorism prior to deployment of Marine troops.

The most productive and significant AT education programs are sponsored by the Air Force and the Army. The Air Force began AT education in 1977, with its Dynamics of International Terrorism (DIT) course at the USAF Special Operations School (USAFSOS), Hurlburt Field, Florida. This five-day awareness course is open to all military services and U.S. government agencies, but the majority of students are Air Force personnel. DIT reaches approximately 800 students per year at the USAFSOS facility[13] and is the only course of its type within the

---

[12] Whereas the Air Force AFOSI handles all the major Air Force investigative functions, the Army separates its intelligence and counterintelligence functions from criminal investigations (Military Intelligence vs. CID).

[13] The USAFSOS usually conducts several tutorial versions of DIT each year at airbases whose personnel need terrorism awareness training but cannot attend the regular course.

Department of Defense. Its purpose, as stated in the USAFSOS Catalog, is to provide "selected military personnel and U.S. Government civilian employees with a basic understanding of the theory, psychology, organization, techniques, and operational capabilities of terrorist groups."[14] The course is intended for military personnel assigned to high-threat areas, who therefore need a high level of awareness about terrorism. Because this is the only such course currently available in the DOD, the other services have expressed concern about the lack of quotas for their personnel. Concurrently, the Air Force has increased its own attendance level, cutting back further other services' and agencies' quotas. As a result, the Army is considering offering a DIT-like course of its own.

The Army began a special five-day terrorism course in 1981 at the Military Police School, Fort McClellan, Alabama. This course, titled "Countering Terrorism on U.S. Army Installations," is taught ten times a year. Unlike the broad-brush treatment of DIT, the Army course is intended to assist installation commanders in protecting their bases against terrorism and preparing for the crisis-management and decisionmaking problems inherent in terrorist incidents.

While other military education programs address some issues of terrorism as part of their curricula, the Air Force and Army courses are the only two specifically devoted to understanding and countering terrorism. Some advanced military education programs, such those at the Army Command and General Staff College, the Air University, and the Navy War College do, however, offer limited instruction in terrorism awareness and understanding as part of their regular curriculums.

Instruction in hostage survival techniques overlaps both education and training. The need for special peacetime hostage-situation guidance (as opposed to wartime Prisoner of War guidance outlined in the Code of Conduct) was first seriously addressed when the U.S. embassy in Tehran was overrun in November 1979 and its staff was taken hostage. A series of cross-service meetings to address this need were held in early 1980, but the Navy refused to deviate from the Code of Conduct in peacetime situations, seeing no need for special guidance. The other services,

---

[14]U.S. Air Force Special Operations School, *Catalog,* Hurlburt Field, Florida, 1984, p. 41.

primarily the Air Force, saw peacetime hostages as unique individuals who are indeed in need of special guidance. The Air Force, as Executive Agent for Code of Conduct training for the Department of Defense, became the first, and as yet the only, service to publish special peacetime standards for its forces.

The Air Force encourages personnel held hostage to interact and develop rapport with their captors to lessen their own symbolic value and thereby become more human in their captors' eyes. The theory behind this training is that a human being is less likely to be killed or mistreated than a symbol. This is a significant departure from the Code of Conduct, which says that POWs are required to give only name, rank, serial number, and date of birth to their captors. Another major area of variance concerns escape: The Code says a POW must make every effort to escape. By comparison, Air Force hostage survival guidance discourages peacetime escape attempts as too dangerous and something to be attempted only as a last resort.

Presently, there are only two major sources of hostage survival education: the DIT course in Florida, and presentations to military and government audiences by an Air Force Intelligence Service representative who specializes in hostage survival. There is some planning within the Air Force to reach larger audiences, but final action has not been completed, and the other three services have not yet codified their thinking on peacetime hostage guidance.

Another element lacking central direction is equipment and devices. However, in this case, centralization may not be critical, since the private sector seems sufficiently productive to satisfy most service needs for special equipment. The Marine Corps has taken the lead from the Army and the Air Force in this regard by providing substantial support for changes in U.S. military small arms.[15] The Marines' displeasure with the M16A1 rifle is a long-standing grievance, and they have sought improvements in this and other military small arms. Several new small-arms systems (including the M16A2 rifle) may be entering

---

[15]Edward Ezell, "USMC Adopts M16A2 Rifle, M60E3 GPMG," *International Defense Review*, No. 12, 1983, p. 1763.

military inventories soon; they undoubtedly will have AT and CT uses in addition to their more conventional functions. These new systems include an updated M16 rifle, a new combat shotgun with a lethal range of 150 meters, and a new 9mm handgun.

Many recent small-arms developments have a decidedly European flavor, since most advances come from Belgium's *Fabrique Nationale* and West Germany's Heckler and Koch. These two companies dominate NATO and U.S. R&D procurement.[16] The U.S. effort primarily involves upgrading weapons originally developed in the 1960s, rather than designing new weapons. New small arms coming into military inventories in the next few years will most likely bear European manufacturing marks (the new M16 rifle being a notable exception).

As outlined in Sec. II, military physical security problems were targeted by the GAO and the Congress for special comment. Programs are under way to address some of these issues. The Army, for example, is upgrading the security of its tactical nuclear storage sites in Europe because of increased concern over terrorism.[17] That program, called the Weapons Access Delay System (WADS), is multifaceted and is designed to deter and defeat assaults against U.S. nuclear assets in Europe.

The Navy, with both seagoing and land-based assets, has some unique physical security problems. In response to the threat of seagoing assaults against its ships, the Navy, primarily through efforts at CINCLANT at Norfolk, Virginia, has begun special small-arms training programs to aid in repelling hostile boarders. This threat is a real one. In 1978, the FBI arrested three people for plotting to board and steal the nuclear submarine USS Trepang. While not planned by political terrorists in the true sense of the term, the plot allegedly involved killing the ship's crew, setting out to sea, and firing a nuclear missile at a U.S. city. The ultimate goal was apparently to sell the submarine to an undisclosed buyer.[18]

---

[16]"Small Arms for the Eighties' Kind of Army," *Defense and Foreign Affairs Digest,* January 1984, pp. 16-18, 31.

[17]Walter Pincus, "Army Spending $35 Million To Protect Nuclear Arsenal," *Washington Post,* January 26, 1984.

[18]Merle MacBain, "Will Terrorism Go to Sea?," *Sea Power,* January 1980, pp. 15-24.

The Navy has undertaken a variety of other initiatives to improve its countermeasures capability. While a recent Rand study concluded that "terrorist attacks on maritime targets are not inevitable,"[19] the upward trend of U.S. military targeting by terrorists indicates that further attention should be devoted to the maritime threat. Although data in the Rand Chronology suggest that terrorists possess limited naval attack capabilities, they do have a wide variety of targets as well as a wide range of weaponry.[20]

---

[19]Brian Michael Jenkins, et al., *A Chronology of Terrorist Attacks and Other Criminal Actions Against Maritime Targets,* The Rand Corporation, P-6906, September 1983.

[20]From 1960 through August 1983, terrorists attacked 47 ships, hijacked 11, and sank or destroyed 12. Weapons have included limpet mines, rockets launched from small boats, and an explosives-filled freighter armed with 122mm rockets. A limited number of groups seem willing or able to take on maritime targets: Cuban emigres, Palestinians, and Irish Republican Army personnel carried out 40 percent of these actions.

V. THE FUTURE OF MILITARY COUNTERMEASURES

If the DOD and the four military services are to be able to respond effectively to terrorism, terrorist trends must be accurately anticipated. If the future holds no change in the *status quo* with respect to either the amount or quality of terrorist activity, there may be little need for innovative action either unilaterally or bilaterally on the part of the services. Current CT and AT programs may be adequate for the current and projected level of threat. However, if the effectiveness and quality of terrorist operations improves, as statistics and research seem to indicate will happen, then flexibility and foresight will be called for in the years ahead.

The argument over terrorism's future threat has already begun. It has been noted that "some members of the U.S. military and the intelligence community feel that an over-concentration on terrorism will divert resources needed for what they deem more important defense and intelligence programs."[1] Some would view this as an argument between parochial program managers interested only in "empire building," but that view seems short-sighted in light of the budget limitations placed on the many programs that affect the entire U.S. military preparedness effort. Terrorism is *not* the only target of intelligence operations; it is *not* the only topic taught in military schools; it is *not* the only threat for which special tactics must be developed; and it is *not* the only threat calling for R&D effort. However, it is a threat that can not be treated lightly or dismissed as an occasional irritant. The 241 Marines killed in the Beirut terrorist attack illustrate that point.

Two recently published documents stress that terrorism is changing or soon may change, to the detriment of Western democracies. The first, published in June 1983, forecasts an ill wind for the U.S. military:

> The three components of armed conflict--conventional war, guerrilla warfare, and terrorism--will coexist in the future, with both governments and subnational entities employing them individually, interchangeably, sequentially, or

[1]Simpson, op. cit., p. 33.

> simultaneously, as well as being required to combat them. Terrorist tactics may be used to publicize the existence of guerrilla groups and finance guerrilla campaigns. Terrorist operations may be substituted when guerrilla warfare fails, or they may be employed as a mode of surrogate warfare by nations unable or unwilling to achieve their aims through diplomacy or conventional military means. Acts of terrorism may accompany conventional warfare between nations.[2]

The second, more recent document is the Long Commission report on the inquiry into the Beirut bombing. The Commission stated that the attack was "an act sponsored by sovereign States or organized political entities," and that such international terrorism, while endemic to the Middle East, is "indicative of an alarming world-wide phenomenon that poses an increasing threat to U.S. personnel and facilities."

If terrorism becomes a major form of armed conflict, the quality of its people and operations is bound to increase. Sponsoring nations bring it the full support of their established intelligence networks, their military education and training facilities, their equipment procurement and supply systems, and the other trappings of government systems. Diplomatic channels are more available for sensitive communications and supply (through diplomatic pouches). Clandestine support networks are more easily tapped to acquire documents, safe houses, transportation, and other support items. State-sponsored terrorists become, in essence, unconventional or irregular military units, carrying the same level of threat as those entities. In the face of this perception, the Long Commission recommended that active programs be implemented to combat this enhanced threat, and that a broad range of military capabilities and options should be made available to meet the increasing challenge.

One active program the Commission recommended was the establishment of an "all-source fusion center, which would tailor and focus all-source intelligence support to U.S. military commanders." At present, each service has its own intelligence/counterintelligence system. In addition, the Defense Intelligence Agency performs intelligence functions for the DOD and the Joint Chiefs of Staff, but the lack of specific warnings from any agency prior to the Beirut bombing points up

---

[2]Jenkins, *New Modes of Conflict*, p. 16.

the need for an all-source intelligence center devoted to the collection, analysis, and dissemination of timely intelligence information.

Another Commission finding and recommendation transcended both AT and CT. The report found that "much needs to be done to prepare U.S. military forces to defend against and counter terrorism" and recommended that the DOD develop the doctrine, planning, organization, forces, and education and training necessary to meet that goal. Many students of the Pentagon scene have noted that interest in AT and CT matters tends to rise and fall depending on the elapsed time since the most recent antimilitary terrorist act. However, Beirut, with its horrendous damage and casualties, seems to have provided continuing impetus for service initiatives to improve countermeasures capabilities.

If the U.S. military is to be an effective element in national terrorism countermeasures initiatives, it must protect and safeguard its limited assets. To better perform internal security functions, joint-service projects would seem to have potential for all the services. But as indicated in the 1981 GAO and Long Commission reports, the initiative to begin centralization and organization efforts must come from the DOD.

BIBLIOGRAPHY

"AFOSI's Counterintelligence Program: Tailor Made," *TIG Brief,* November 29, 1982, pp. 1-2.

Air Force Regulation 208-1, *The U.S. Air Force Antiterrorism Program,* October 25, 1982.

Bornmann, Karl Gerhard, "Modern Weapons and Equipment Increase the Striking Power of Counterterrorist Groups," *Military Technology,* August 1982, pp. 155-160.

Boyd, Gerald W., "Special Weapons and Tactics Teams: A Systems Approach," *FBI Law Enforcement Bulletin,* September 1977, pp. 21-26.

Bruchey, William J., Jr., *Ammunition for Law Enforcement: Part I, Methodology for Evaluating Relative Stopping Power, and Results,* Ballistic Research Laboratory, Aberdeen Proving Ground, Technical Report ARBRL-TR-02199, October 1979.

The Budget of the United States Government, Fiscal Year 1980, U.S. Government Printing Office, Washington, D.C., 1979.

Defense Needs Better System for Assuring Adequate Security at Reasonable Cost on U.S. Bases, General Accounting Office, Report to the Congress, PLRD-81-1, March 6, 1981.

"Emergency Service Teams-HQ USAF," *TIG Brief,* May 16, 1983.

Ezell, Edward, "USMC Adopts M16A2 Rifle, M60E3 GPMG," *International Defense Review,* No. 12, 1983, pp. 1763-1764.

Jenkins, Brian Michael, *New Modes of Conflict,* The Rand Corporation, R-3009-DNA, June 1983.

———, et al., *A Chronology of Terrorist Attacks and Other Criminal Actions Against Maritime Targets,* The Rand Corporation, P-6906, September 1983.

Johnson, Paul, "The Seven Deadly Sins of Terrorism," *NATO Review,* Vol. 28, No. 5, October 1980, pp. 28-33.

"LASIII Laser Aiming Point," *International Defense Review,* No. 10, 1983, p. 1471.

MacBain, Merle, "Will Terrorism Go to Sea?," *Sea Power,* January 1980, pp. 15-24.

Pattakos, Arion N., "OPSEC--Operations Security at DoD," *Security Management,* November 1983, pp. 102-105.

Physical Security at U.S. Military Bases, Hearing Before the Investigations Subcommittee of the House Committee on Armed Services, 97th Cong., 1st Sess., July 17, 1981.

Physical Security at U.S. Military Bases, Report of the Investigations Subcommittee of the House Committee on Armed Services, 97th Cong., 1st Sess., November 5, 1981.

Pincus, Walter, "Army Spending $35 Million To Protect Nuclear Arsenal," *Washington Post,* January 26, 1984.

Report of the DOD Commission on Beirut International Airport Terrorist Act, October 23, 1983, December 20, 1983.

Schoch, Bruce P., "Four Rules for a Successful Rescue," *Army,* February 1981, pp. 22-25.

Simpson, Howard R., "Organizing for Counter-Terrorism," *Strategic Review,* Winter 1982, pp. 28-33.

"Small Arms for the Eighties' Kind of Army," *Defense and Foreign Affairs Digest,* January 1984, pp. 16-18, 31.

Statistical Abstract of the United States, 1980, 101st Edition, Bureau of the Census, U.S. Government Printing Office, Washington, D.C., 1980.

Time, April 13, 1981, p. 29.

U.S. Air Force Special Operations School, *Catalog,* Hurlburt Field, Florida, 1984.

U.S. Army Training Circular TC 19-16, *Countering Terrorism on U.S. Army Installations,* Aril 25, 1983.

"Very-high-velocity Small-arms Ammunition," *International Defense Review,* No. 10, 1983, p. 1471.

END

FILMED

5-85

DTIC